

REMARKS

This responds to the Office Action mailed on October 5, 2006, and the references cited therewith.

Claims 62 and 64-66 are amended, no claims are canceled, and no claims are added; as a result, claims 1-3, 6-9, 21-28, 62-69 and 85 are now pending in this application.

§103 Rejection of the Claims

Claims 1-6, 8-9, 21-28, 62-69 and 85 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Win et al. (U.S. 6,453,353, hereinafter “Win”) in view of Duvvoori et al. (U.S. 6,021,438, hereinafter “Duvvoori”).

Applicants respectfully submit that the Office Action did not make out a *prima facie* case of obviousness for the following reasons:

Even if combined, the cited references fail to teach or suggest all of the elements of applicants’ claimed invention;

The reference (or references when combined) must teach or suggest all the claim elements. M.P.E.P. § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir. 1991)).

Claim 1 recites:

A method to provide access to services of an online commerce site that includes a plurality of servers, the method comprising:
receiving an access request from a client, the access request including an API function call;
identifying an API server of the plurality of servers to which to direct the client for service by the online commerce site;
generating an access rule associated with the client, the API function call, and the API server; and
transmitting the access rule to the client. (Emphasis Added)

Win is directed at a method and system to provide a user access to authorized Web resources, based on the user’s role in the organization that controls the Web resources. The information resources are stored on a protected Web server. A user of a client or browser logs in to the system. A runtime module on the protected server receives the login request and intercepts all other requests by the client to use a resource. The runtime module connects to an access

server that can determine whether a particular user is authentic and which resources the user is authorized to access. User information is associated with roles and functional groups of an organization to which the user belongs; the roles are associated with access privileges. . . . The user is presented with a customized Web page showing only those resources that the user may access. (Win, Abstract) The office Action cites the following quotes from the reference:

"The system 2 enables administrators to implement access rules by defining Roles that Users play when working for an organization or doing business with an enterprise. A Role may reflect a relationship of a User to the organization (employee, customer, distributor, supplier), their department within an organization (sales, marketing, engineering) or any other affiliation or function (member of quality task force, hotline staff member) that defines their information needs and thus their access rights or privileges. Thus, examples of Roles include Employee, Customer, Distributor, Supplier, Sales, Marketing, Engineering, and Hotline Staff."

(Win, Col. 5, lines 21-32) (Emphasis Added)

In the above quote Win describes the role that a user may play in the organization the resources of which the user is trying to access. The system in Win then enables the administrator to implement access rules by defining the roles.

"An administrator may create an association of a role with one or more resources, in Registry Repository 110 . . . In response, Administration Application displays a role assignment display for the selected resource. . . . The title of display 1020, "Assigning Roles to National Sales Report," indicates that the user selected the resource "National Sales Report" To create an association of a role to the selected resource, a user selects one of the roles 1028a-1028n from the list 1026 and selects the Assign button 1036. In response, Administration Application 114 displays the selected role (such as "Sales Manager") in the assigned roles list 1024. The user or administrator may make the displayed association persistent . . . In response, Administration Application creates an association of the "Sales Manager" role to the "National Sales Report" resource and stores the association in the database."

(Win, Col. 18, lines 1-27) (Emphasis Added)

According to the above quote, an administrator in Win creates an association of roles with resources, such that each user may only use certain resources based on the role the user plays in the organization. The user may select a resource and then create an association of a role to the selected resource by choosing one of the roles from a list of roles presented to the user. However, in the above quotes is silent on generation of access rules and any association of the access rules with the API function call and the API server, as required by claim 1. In other words, Win does not teach "generating an access

rule associated with the client, the API function call, and the API server.” as recited in claim 1. The Office Action alleges that Win discloses “transmitting the access rule to the client” and cites the following quote:

“Access Server 106 stores a log-in page, Authentication Client Module and Access Menu Module. The Authentication Client Module authenticates a user by verifying the name and password with the Registry Server 108. If the name and password are correct, the Authentication Client Module reads the user's roles from the Registry Server 108. It then encrypts and sends this information in a "cookie" to the user's browser. A "cookie" is a packet of data sent by web servers to web browsers. Each cookie is saved by browser 100 until the cookie expires. Cookies received from a web server in a specific domain are returned to web servers in that same domain during open URL requests. A cookie returned by the Authentication Client Module is required for access to resources protected by the system 2.”

(Win, Col. 6, lines 41-54) (Emphasis Added)

Based on the above quote, Win sends a cookie containing encrypted user's roles to the user's browser. However, Win does not teach “*transmitting the access rule to the client,*” as recited by claim 1.

Duvvoori is directed at a license restriction management system having wrapper programs and agents as appropriate to manage launches of application programs in distributed systems of computers having a multiplicity of different operating systems. (Duvvoori, Abstract) The Office Action, at page 3, paragraph 1, asserts that Win does not teach that the user's request including API function call. The Examiner then cites the following quotes from the reference:

“When this DLL 138 is loaded, the 32-bit agent service detects this fact in step 146, and determines the handle of the 32-bit application that was launched . . . The handle of the application program can be simply a number which is unique to the particular application, or it can be a collection of the application program's ID, the user ID of the user who launched it, the size of the application, the machine ID on which it was launched, and the time of the launch. This handle information is kept by the Windows NT operating system and is made available to the 32-bit agent service by invoking a plurality of function calls of a public API of the NT operating system to request the information. In the preferred embodiment, the 32-bit agent service invokes a first API function call to obtain the application process ID and then invokes other API functions to obtain the other information of the handle for use in composing the license request message to the LRMP. . . .”

(Col. 15, lines 17-43) (Emphasis Added)

According to the above passage, the 32-bit agent invokes API function calls to receive information about the application program's ID, user's ID, etc.

"... if the handle determined in step 146 is the handle of a VDM 32-bit emulation process, processing branches to ... the process of the 32-bit agent participating in the creation by Windows NT of the virtual computer by injecting therein an API ... This API provides availability of function calls which can be invoked by 32-bit agent service ... to request a 16-bit agent process ... to determine the handles of any 16-bit applications running inside the virtual computer 150. The API also provides another function call which may be invoked by the 32-bit agent service 96 to request the 16-bit agent service to terminate the execution of specified 16-bit application processes. Each VDM that is created by Windows NT is altered in this way by the 32-bit agent process so as to have such an API and to have a 16-bit agent which starts up with the start up of the emulator program which creates the virtual machine. ... The 16-bit agent 173 is modified from the prior art 16-bit agents in that it has no capability to communicate directly with the LRMP process using either TCP or UDP communication protocols ... and it has the ability to respond to function calls made to the API 171 by the 32-bit agent process in the manner described below. . . ."

(Col. 16, lines 16-56) (Emphasis Added)

The above quote describes the API providing function calls to be invoked by the 32-bit agent to request information about the 16-bit applications running inside the virtual machine; or to request the 16-bit agent to terminate the execution of a 16-bit application. However, the function calls in Duvvoori are not *"API function calls included in an access request"* received from a client, as required by claim 1. Moreover, Duvvoori fails to teach *"generating an access rule associated with the client, the API function call, and the API server,"* and *"transmitting the access rule to the client,"* as recited in claim 1 and not taught by Win. As such, Win and Duvvoori, independently or in combination, fail to teach or suggest each and every limitations of claim 1. Therefore, Applicants respectfully submit that, at least for the above reasons, claim 1 is not rendered obvious by the combination; thus it is allowable. Claims 2-3, 6, 8-9, 23-25 are dependent on claim 1, thus at least for the same reasons set forth above are allowable and their rejections under 35 U.S.C. § 103(a) should be withdrawn.

The same arguments as presented with respect to claim 1 are also applicable to a consideration of independent claims 62 and 85; thus, at least for the same reasons set forth above, independent claims 62 and 85, and dependent claims 63-69, depending from

claim 62, are allowable and it is requested that their rejection under 35 U.S.C. § 103(a) be withdrawn.

Claim 21 recites the following limitations:

receiving a service request from a client for access to a service on an API server supporting the online commerce site, the service request including at least a portion of an access rule associated with the client, an API function call, and the API server, the access rule having been previously provided to the client by the online commerce site; and
validating the service request based on the access rule.

Based on the above analysis of the references, Win and Duvvoori, independently or in combination, do not teach “service request including at least a portion of an access rule associated with the client, an API function call, and the API server, the access rule having been previously provided to the client by the online commerce site,” as recited in claim 21. As such, the references fail to teach each and every elements of claim 21 and do not render the claim obvious. Thus, at least for the reason noted above, claim 21 and its dependent claims 22 and 26-28 are allowable. Therefore, Applicants respectfully request that the rejection of claims 21, 22 and 26-28 under 35 U.S.C. § 103(a) be withdrawn.

CONCLUSION

Applicants respectfully submit that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicants' attorney at 408-406-4855 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

SCOTT LEAHY ET AL.

By their Representatives,

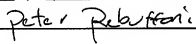
SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
408-406-4855

Date 04/05/2007

By 

Jim H. Salter
Reg. No. 35,668

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 5 day of April 2007.


Name


Signature